

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение
высшего образования
«Национальный исследовательский ядерный университет
«МИФИ»

ДОМАШНЕЕ ЗАДАНИЕ №1:
«Оценка пропускной способности скрытых каналов»

По дисциплине «Защита информации от утечки по скрытым
каналам»

Выполнил студент группы Б19-515
Щербакова Александра

Москва, 2023 г.

Случай 1.

Найти N , при котором пропускная способность скрытого канала будет максимальной.

Вероятности входных символов	Ошибки в канале
Вероятности входных символов одинаковы и равны $1/N$	Канал без ошибок (символы передаются с вероятностью, равной 1).

Дан скрытый канал, передающий N символов. На передачу символа « i » требуется i секунд (к примеру, на передачу символа «1» требуется 1 секунда, на передачу символа «2» требуется 2 секунды, и так далее).

Формула для вычисления пропускной способности:

$$v = \max_X \left\{ \frac{I(X, Y)}{\tau} \right\},$$

где:

- $\tau = \frac{\sum_{i=1}^n i}{n} = \frac{0,5n(n+1)}{n} = 0,5(n + 1)$ — среднее время передачи одного пакета
- $I(X, Y) = H(Y) - H(Y|X)$ — взаимная информация случайных величин X и Y
- $H(Y) = -\sum_{i=1}^n p_{\text{вых}}(i) \log_2 p_{\text{вых}}(i)$ — энтропия случайной величины Y
- $H(Y|X) = 0$ — условная энтропия случайной величины Y относительно случайной величины X (равна нулю, так как канал по условию без ошибок)
- $p_{\text{вых}}(i) = \frac{1}{n}$ — вероятность распознавания получателем символа « i » (по условию все символы равновероятны)

Код на Python для вычисления пропускной способности и построения графика:

```
import math
import matplotlib.pyplot as plt
```

```

def bandwidth(n):
    hy = 0
    for i in range(1, n + 1):
        hy += ((1 / n) * math.log2(1 / n))
    t = 0.5 * (n + 1)
    return -hy / t

if __name__ == "__main__":
    bw = 0
    n_final = 0
    bw_array = []
    n_array = []

    for n in range(1, 30):
        bw_tmp = bandwidth(n)
        if bw_tmp > bw:
            bw = bw_tmp
            n_final = n
        bw_array.append(bw_tmp)
        n_array.append(n)

    print("Максимальная пропускная способность = ",
bw)
    print("Число пакетов = ", n_final)

    plt.suptitle('График зависимости пропускной
способности скрытого канала от числа пакетов')
    plt.xlabel('N - Число пакетов')
    plt.ylabel('Пропускная способность')
    plt.xticks(n_array)
    plt.plot(n_array, bw_array)
    plt.scatter(n_final, bw, color='red', marker='o')
    plt.show()

```

Результат:

Максимальная пропускная способность = 0.8

Число пакетов = 4

Построить график зависимости пропускной способности скрытого канала от N .



Случай 2.

Найти N , при котором пропускная способность скрытого канала будет максимальной.

2	Вероятности входных символов одинаковы и равны $1/N$	Канал с ошибками. <ul style="list-style-type: none">• $p(i-1 i) = 0.2, p(i i) = 0.6, p(i+1 i) = 0.2, i = \overline{2, N-1}$• $p(N 1) = 0.2, p(1 1) = 0.6, p(2 1) = 0.2$• $p(N-1 N) = 0.2, p(N N) = 0.6, p(1 N) = 0.2$
---	--	--

Формула для вычисления пропускной способности:

$$v = \max_x \left\{ \frac{I(X, Y)}{\tau} \right\},$$

где:

- $\tau = \frac{\sum_{i=1}^n i}{n} = \frac{0,5n(n+1)}{n} = 0,5(n + 1)$ — среднее время передачи одного пакета
- $I(X, Y) = H(Y) - H(Y|X)$ — взаимная информация случайных величин X и Y
- $H(Y) = -\sum_{i=1}^n p_{\text{вых}}(i) \log_2 p_{\text{вых}}(i)$ — энтропия случайной величины Y
- $H(Y|X) = -\sum_{j=1}^n p_{\text{вх}}(j) (\sum_{i=1}^n p_{\text{вых}}(i|j) \log_2 p_{\text{вых}}(i|j))$ — условная энтропия случайной величины Y относительно случайной величины X
- $p_{\text{вх}}(j)$ — вероятность отправки символа «j»
- $p_{\text{вых}}(i) = \frac{1}{n}$ — вероятность распознавания получателем символа «i» (по условию все символы равновероятны)
- $p_{\text{вых}}(i|j)$ — условная вероятность распознавания получателем символа «i» при отправке символа «j». Даны по условию задачи. Случаи, не описанные в условии задачи - равновероятно

Код на Python для вычисления пропускной способности:

```
def bandwidth_with_errors(n):
    t = (n + 1) / 2
    h = 0
    for j in range(1, n + 1):
        h_y_x = 0
        h_ex = 0
        for i in range(1, n + 1):
            h_ex = 0
            if j == i:
                h_ex += 0.6 * math.log2(0.6) * (-1)
            elif j == (i - 1) or j == (i + 1):
                h_ex += 0.2 * math.log2(0.2) * (-1)
            else:
                h_ex += (1/j) * math.log2(1/j) * (-1)
            h_y_x = (-1) * (1/i) * h_ex
        h += ((1 / n) * math.log2(1 / n)) * (-1) - h_y_x
    banw = h / t
    return banw
```

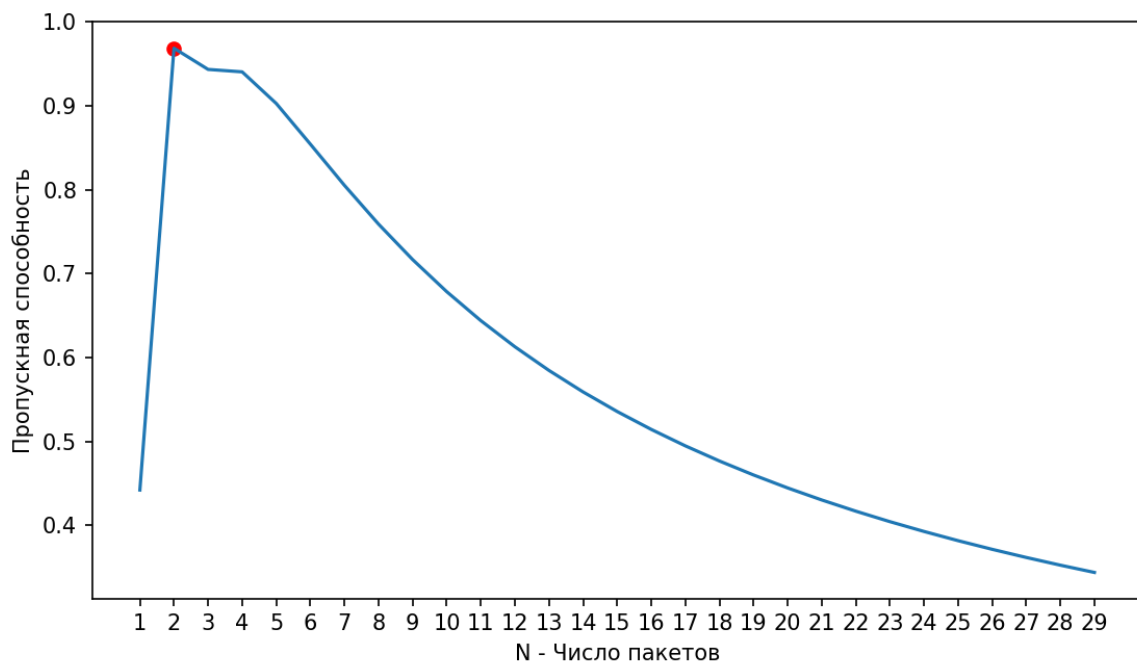
Результат:

Максимальная пропускная способность = 0.9688549918257321

Число пакетов = 2

Построить график зависимости пропускной способности скрытого канала от N .

График зависимости пропускной способности скрытого канала от числа пакетов



Случай 3.

Найти N , при котором пропускная способность скрытого канала будет максимальной.

3	Вероятности входных символов равны: $p(i) = \frac{1}{2^i}$.	Канал без ошибок (символы передаются с вероятностью, равной 1).
---	--	---

Дан скрытый канал, передающий N символов. На передачу символа « i » требуется i секунд (к примеру, на передачу символа «1» требуется 1 секунда, на передачу символа «2» требуется 2 секунды, и так далее).

Формула для вычисления пропускной способности:

$$v = \max_X \left\{ \frac{I(X, Y)}{\tau} \right\},$$

где:

- $\tau = \frac{\sum_{i=1}^n i}{n} = \frac{0,5n(n+1)}{n} = 0,5(n + 1)$ — среднее время передачи одного пакета
- $I(X, Y) = H(Y) - H(Y|X)$ — взаимная информация случайных величин X и Y
- $H(Y) = -\sum_{i=1}^n p_{\text{вых}}(i) \log_2 p_{\text{вых}}(i)$ — энтропия случайной величины Y
- $H(Y|X) = 0$ — условная энтропия случайной величины Y относительно случайной величины X (равна нулю, так как канал по условию без ошибок)
- $p_{\text{вых}}(i) = \frac{1}{2^i}$ — вероятность распознавания получателем символа «i» (по условию все символы равновероятны)

Код на Python для вычисления пропускной способности и построения графика:

```
def bandwidth_with_probability(n):
    t = (n + 1) / 2
    h = 0
    for n_tmp in range(1, n + 1):
        h += ((1 / 2 ** n_tmp) * math.log2(1 / 2 ** n_tmp)) *
    (-1)
    banw = h / t
    return banw
```

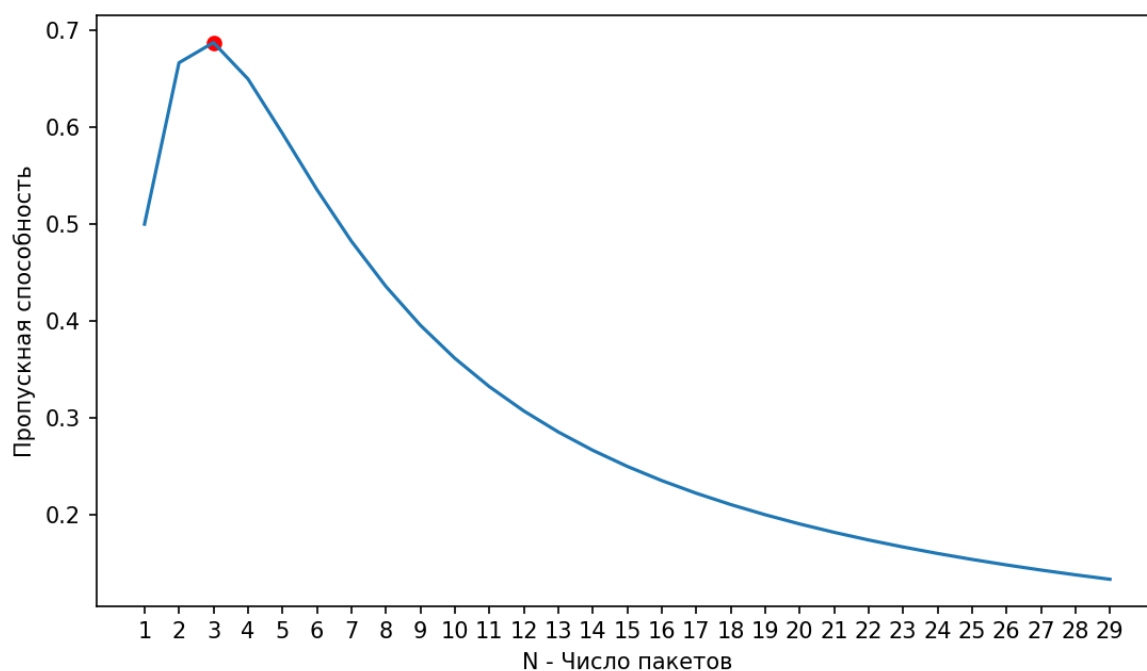
Результат:

Максимальная пропускная способность = 0.6875

Число пакетов = 3

Построить график зависимости пропускной способности скрытого канала от N.

График зависимости пропускной способности скрытого канала от числа пакетов



Заключение

В ходе выполнения работы получен навык вычисления пропускной способности каналов с ошибками и без. Применялся подход, основанный на оценке взаимной информации случайных величин X и Y , описывающих входные и выходные характеристики скрытого канала.

Построены графики зависимости пропускной способности скрытых каналов от числа пакетов. Из результатов работы можно сделать следующий вывод: максимальная пропускная способность достигается при малой длине сообщения.